FAA-STD-045
November 21, 1994

U.S. Department of Transportation

Federal Aviation Administration

Standard

National Airspace System (NAS)

Open Systems Interconnection Security Architecture, Protocols and Mechanisms

FOREWORD

This standard establishes the security architecture, protocols and mechanisms to be used with the National Airspace System (NAS) data communications architecture for the provision of secure communications between NAS Open Systems Interconnection (OSI) systems. The security architecture described in this standard is based on the Basic Reference Model OSI security Architecture as defined in the International Organization for Standardization (ISO) standard ISO 7498-2

The NAS will consist of various types of processors and communication network sub-systems procured from a variety of vendors. A well defined security architecture and security mechanisms are required to ensure that NAS operational systems are protected at the level required by the FAA Telecommunications and Automated Information Security Policy Orders.

Table of Contents

Appendix

Figure Title Page No.

Table Title Page No.

1. SCOPE

1.1 Scope

This standard specifies a minimum set of security services, protocols and mechanisms required to meet the NAS security requirements as identified in FAA order 1600.54B, FAA order 1600.66, DoD 5200.28-std and NAS-SR-1000. Additional security services and mechanisms may be required for specific information exchanges between NAS end-systems and others. These additional services shall be implemented through mutual agreements which are in accordance with FAA NAS security policies.

The focus of this standard is the secure communication between any combination of NAS end-systems and NAS intermediate systems that are interconnected using the OSI protocols as specified in FAA-STD-39. This security standard addresses protection of access to the NAS system via its OSI interface. It also addresses protection of data that is carried via OSI protocols between NAS systems.

This standard does not address protection of the NAS OSI systems from external threats using non-OSI protocols which may be supported by the system or internal threats due to staff operating outside of NAS security policies and procedures for computer processing and communications equipment.

1.2 Purpose

The purpose of this standard is to establish a uniform approach to implementing security services protocols and mechanisms in NAS end-systems, wide area networks and local area networks. This will allow secure interoperability between NAS OSI systems that are required to communicate.

The communications security architecture, services and mechanisms described herein shall be used in the development of interface requirements as part of the overall data communications planning, design and procurement of the NAS.

1.3 Relationship to Other Documents

The security architecture, mechanism and services called out in the standard are aligned with the NAS communications security requirements derived from the following documents: FAA order 1600.54B, FAA order 1600.66, DoD 5200.28-std, NAS-SR-1000 and the International Civil Aviation Organization (ICAO) Aeronautical Telecommunications Network (ATN) manual.

This standard places operational and technical requirements on the future implementation of an OSI compliant FAA network management service (see section 3.2.8). These requirements must be fully addressed in the FAA Network Management standard for it to provide sufficient functionality to complement and support the NAS open system security architecture.

2. APPLICABLE DOCUMENTS

The following documents form a part of this standard to the extent specified herein. In the event of conflict between the documents referenced herein and the contents of this standard, the contents of this standard shall take precedence.

2.1 Government Documents

FAA Standards

FAA-STD-039(a)	National Airspace System (NAS) Open Systems Architecture and Protocols, October 27, 1993
FAA-STD-042	National Airspace System (NAS) Open Systems Interconnection (OSI) Naming and Addressing, January 9, 1992
FAA-STD-047	National Airspace System (NAS) Open Systems Interconnection (OSI) Conformance Testing, December 29, 1993

FAA Orders

FAA Order 1600.54B:2-7-89	Automated Information Systems Security Handbook
FAA Order 1600.66 :final clearance draft	Telecommunications and Information Systems Security Policy

National Airspace System Documents

NAS-SR-1000	National Airspace System, System Requirements Specification

Federal Standards

DOD 5200.28-STD:8-15-83	Department of Defense Trusted Computer System Evaluation Criteria (Orange Book)

National Institute of Standards and Technology

SP-500-214	Stable Implementation Agreements for Open Systems Interconnection Protocols Version 7 Edition 1

2.2 Non-Government Documents

International Civil Aviation Organization (ICAO)

Aeronautical Telecommunication Network Manual Edition 2 :November 19 1994

International Organization for Standardization (ISO)

ISO 7498-2:1989	Information processing systems - Open System Interconnection Basic Reference Model Part 2: Security Model.
ISO 8072:1986	Information processing systems - Open System Interconnection - Transport Service Definition, 1st Edition.
ISO 8073:1992	Information Processing Systems, Open Systems Interconnection, Connection Oriented Transport Protocol Specification, 3rd Edition
ISO 8073/AD2:1989	Information Processing Systems - Open Systems Interconnection Connection Oriented Transport Protocol Specification - Addendum 2: Class Four Operation Over Connectionless Network Service.
ISO 8202:1990	Information Processing Systems - Data Communications - X.25 Packet Level Protocol for Data Terminal Equipment, 2nd Edition.
ISO 8473-1:1994	Information processing systems - Open Systems Interconnection Protocol for Providing the Connectionless-Mode Network Service - Part 1: Protocol Specification.
ISO 8473-2:1994	Information processing systems - Open Systems Interconnection Protocol for Providing the Connectionless-Mode Network Service - Part 2: Provision of the underlying service by an ISO/IEC 8802 subnetwork.
ISO 8473-3:1994	Information processing systems - Open Systems Interconnection Protocol for Providing the Connectionless-Mode Network Service - Part 3: Provision of the underlying service by an X.25 subnetwork.
ISO 8473-4:1994	Information processing systems - Open Systems Interconnection Protocol for Providing the Connectionless-Mode Network Service - Part 4: Provision of the underlying service by a subnetwork that provides the OSI data link service.

ISO 8327:1987	Information processing systems - Open System Interconnection Basic connection oriented session protocol specification.
ISO 8571-1:1988	Information Processing Systems - Open Systems Interconnection - File Transfer. Access. and Management - Part 1: General Introduction. 1st Edition
ISO 8571-2:1988	Information Processing Systems - Open Systems Interconnection - File Transfer, Access, and Management - Part 2: Virtual Filestore Definition. 1st Edition
ISO 8571-3:1988	Information Processing Systems - Open Systems Interconnection File Transfer. Access, and Management - Part 3: File Service Definition. 1st Edition
ISO 8571-4:1988	Information Processing Systems - Open Systems Interconnection File Transfer. Access. and Management - Part 4: File Protocol Specification. 1st Edition
ISO 8650:1988	Information processing systems - Open Systems Interconnection Protocol specification for the Association Control Service Element.
ISO/IEC 8802-2:1990	Information processing systems - Local Area Networks - Part 2: Logical Link Control, 1st Edition.
ISO/IEC 8802-3:1990	Information processing systems - Local Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification, 2nd Edition.
ISO/IEC 8802-4:1990	Information processing. systems - Local Area Networks - Part 4: Token-Passing Bus Access Method and Physical Layer Specifications. 1st Edition.
ISO/IEC 8802-5:1990	Information processing systems - Local Area Networks - Part 5: Token Ring Access Method and Physical layer Specification. 1st Edition.
ISO 8823:1988	Information processing systems - Open Systems Interconnection - Connection oriented presentation protocol specification.
ISO 8824:1987	Information processing systems - Open Systems Interconnection Specification of Abstract Syntax Notation One (ASN.1)

ISO 9040:1990	Information processing systems Open Systems Interconnection - Virtual Terminal Basic Class Service. 1st Edition
ISO 9041:1990	Information processing systems Open Systems Interconnection - Virtual Terminal Basic Class Protocol - Part 1: Specification.
ISO 9594-1:1994	Information technology - Open Systems Interconnection - The Directory - Part 1: Overview of Concepts, Models. and Services, 1st Edition
ISO 9594-2:1994	Information technology - Open Systems Interconnection - The Directory - Part 2: Models, 1st Edition
ISO 9594-3:1994	Information technology - Open Systems Interconnection - The Directory - Part 3: Abstract Service Definition, 1st Edition
ISO 9594-4:1994	Information technology - Open Systems Interconnection - The Directory - Part 4: Procedures for Distributed Operations, 1st Edition
ISO 9594-5:1994	Information technology - Open Systems Interconnection - The Directory - Part 5: Protocol Specifications, 1st Edition
ISO 9594-6:1994	Information technology - Open Systems Interconnection - The Directory - Part 6: Selected Attributed Types, 1st Edition
ISO 9594-7:1994	Information technology - Open Systems Interconnection - The Directory - Part 7: Selected Object Classes, 1st Edition
ISO 9594-8:1990	Information technology - Open Systems Interconnection - The Directory - Part 8: Authentication Framework, 1st Edition
ISO/IEC 10021-1:1990	Information Processing - Text Communication - Message Oriented Text Interchange System - Part 1: System and Service Overview
ISO/IEC 10021-2:1990	Information Processing - Text Communication - Message Oriented Text Interchange System - Part 2: Overall Architecture
ISO/IEC 10021-3:1990	Information Processing - Text Communication - Message Oriented Text Interchange System - Part 3: Abstract Service Definition and Procedures

ISO/IEC 10021-4:1990	Information Processing - Text Communication - Message Oriented Text Interchange System - Part 4: Message Transfer System: Abstract Service Definition and Procedure
ISO/IEC 10021-5:1990	Information Processing - Text Communication - Message Oriented Text Interchange System - Part 5: Message Store: Abstract Service Definition
ISO/IEC 10021-6:1990	Information Processing - Text Communication - Message Oriented Text Interchange System - Part 6: Protocol Specification
ISO/IEC 10026-1:1992	Information processing systems Open Systems Interconnection - Distributed Transaction Processing -Part 1: Model
ISO/IEC 10026-2:1992	Information processing systems Open Systems Interconnection-Distributed Transaction Processing -Part 2: Service Definition
ISO/IEC 10026-3:1992	Information processing systems Open Systems Interconnection - Distributed Transaction Processing -Part 3: Protocol Specification
ISO/IEC 10164-8:1993	Information Technology - Open Systems Interconnection Systems Management - Part 8: Security Audit Trail Function
ISO/IEC 10589:1992	Information Technology - Telecommunication and Information Exchange between Systems - Intermediate System (IS) to (IS) -Intra-Domain Routing Information Exchange Protocol for use in conjunction with the Connectionless-mode Network Service
ISO/IEC 10736:1993	Information Technology - Telecommunications and Information Exchange Between Systems - Transport Layer Security Protocol
ISO/IEC 10747	Information Technology - Telecommunications and Information Exchange Between Systems - Protocol Exchange between Systems - Protocol Exchange of Inter-Domain Routing Information among Intermediate Systems to Support forwarding of ISO 8473 PDUs

ISO/IEC 11577:1993	Information Technology - Telecommunications and Information Exchange Between Systems - Network Layer Security Protocol
ISO/IEC 13712-1:1994	Information Technology -Remote Operations -Part 1: Concepts,Model and Notation

Institute of Electrical and Electronic Engineers (IEEE)

IEEE 802.10-B:1992	Standard for Interoperable Local Area Network Security (SILS) Part B Secure Data Exchange
IEEE 802.1a	Local Area Network and Metropolitan Area Network - Overview and Architecture

3. REQUIREMENTS

3.1 General Requirements

This standard defines NAS OSI security requirements in accordance with the OSI seven layer architecture and is aligned with the security model described in the Aeronautical Telecommunication Network (ATN) manual.

It defines the security protocols and mechanisms which shall be used at selected OSI layers to facilitate secure interoperability between OSI systems internal to the NAS and OSI systems which form part of the ATN. The protocols and services are organized within a security architecture to reduce duplication of security services and maximize the level of interoperability between secured systems.

Implementation of security services in NAS OSI systems is a mandatory requirement as defined by the security policies which govern that system (see section 3.1.3).

3.1.1 NAS Open Systems Interconnection Security Architecture

The NAS security architecture sub-divides security services across the Application, Transport, Network and Data Link layers as indicated in table 3.1. The protocols used to provide those services are positioned within terms of the OSI reference model as shown in figure 1. This section describes an overview of the security services and protocols which form the NAS OSI Security Architecture.

3.1.1.1 Transport and Application Layer Security

The Association Control Service Element (ACSE) and the Transport Layer Security Protocol (TLSP) provide the key security services for supporting secure end-system to end-system communications between NAS OSI applications.

At the Application Layer, ACSE offers authentication services to all NAS ASEs. Peer entity authentication, based on the ISO/IEC 9594-8 Authentication Framework, is supported in this architecture. Discretionary access control services are also offered at the Application Layer by those ASEs that support access control services (e.g. Directory Services). Requirements for using Application layer security services are specified in section 3.2.7 of this document.

The Security services offered at the Transport Layer are data integrity and data confidentiality. These two services are provided by the TLSP and use encipherment algorithms to protect data from modification or eavesdropping. Requirements for using Transport Layer security services are specified in section 3.2.4 of this document.

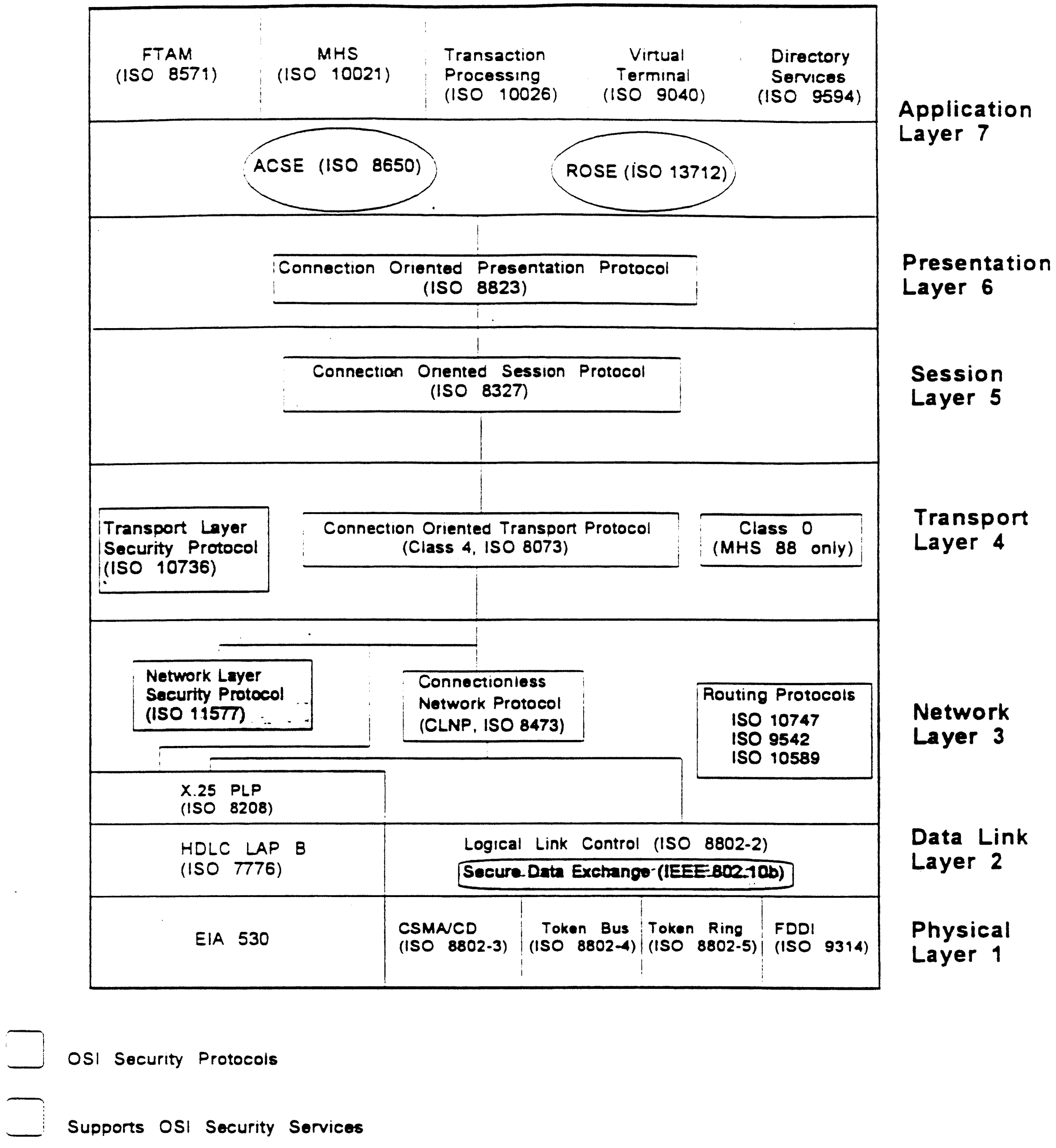

FTAM (ISO 8571)
MHS (ISO 10021)
Transaction Processing (ISO 10026)
Virtual Terminal (ISO 9040)
Directory Services (ISO 9594)
ACSE (ISO 8650)
ROSE (ISO 13712)
Application Layer 7
Connection Oriented Presentation Protocol (ISO 8823)
Presentation Layer 6
Connection Oriented Session Protocol (ISO 8327)
Session Layer 5
Transport Layer Security Protocol (ISO 10736)
Connection Oriented Transport Protocol (Class 4, ISO 8073)
Class 0 (MHS 88 only)
Transport Layer 4
Network Layer Security Protocol (ISO 11577)
Connectionless Network Protocol (CLNP, ISO 8473)
Routing Protocols ISO 10747 ISO 9542 ISO 10589
Network Layer 3
X.25 PLP (ISO 8208)
HDLC LAP B (ISO 7776)
Logical Link Control (ISO 8802-2)
Secure Data Exchange (IEEE 802.10b)
Data Link Layer 2
EIA 530
CSMA/CD (ISO 8802-3)
Token Bus (ISO 8802-4)
Token Ring (ISO 8802-5)
FDDI (ISO 9314)
Physical Layer 1
OSI Security Protocols
Supports OSI Security Services

Figure 1 NAS OSI Architecture and Security Protocols

3.1.1.2 Network and Data Link Layer Security

The Network Layer offers security services related to the use of specific network layer protocols. Within the NAS security architecture, network layer security services are intended to protect access between end-systems and intermediate systems or between two intermediate systems. These services should be differentiated from the end-system to end-system security services discussed in the paragraph above. The ISO 8208 Packet Layer Protocol supports Discretionary Access Services through the implementation of Closed User Groups (CUGs). The Connectionless Network Protocol (CLNP) supports access control mechanisms which, when used in conjunction with IDRP, restricts the routes CLNP traffic may take. This is implemented using Security Labels which comply with the ICAO ATN security services. The Network Layer Security Protocol provides Data Origin Authentication and Data Integrity services between NAS Routers (intermediate systems) within the NAS Internet. Requirements for using Network Layer security services are specified in section 3.2.3 of this document.

At the Data Link Layer, Data Origin Authentication and Data Integrity services are offered by the Secure Data Exchange Protocol (SDE) for use in conjunction with ISO/IEC 8802-2 based local area networks. The requirements for using Data Link layer security services are specified in section 3.2.2 of this document.

3.1.1.3 Selecting a Security Service

The decision to implement a specific service at a selected layer is dependent on the security policy for that security domain (see section 3.1.3), the level of protection required for the information being exchanged and the points within the NAS Internet which are untrusted and may allow an attack on information transfer or end-system operation. The security protocols indicated in figure 1 present options which may be selected from when implementing OSI security services.

Section 3.1.2 describes a partitioned view of the NAS Internet which assists in identifying the untrusted elements of the NAS Internet and deciding appropriate security protocols to select for deployment.

	NAS OSI Security Layers				
NAS Security Services	Data Link Layer IEEE 802.10b	Network Layer ISO 11577 NLSP	ISO 8208 CUG/NUI	Transport Layer ISO 10736	Application Layer ISO 8650, ISO 8571, ISO 10021, ISO 9594
Data Integrity	X	X		X	
Data Confidentiality				X	X
Authentication					X
Audit Trail	X	X		X	X
Discretionary Access Control			X		X
Data origin authentication	X	X			

Table 3.1 Security services supported at each layer of the NAS security architecture

3.1.2 Relationship to NAS WAN, LAN and Router Architectures

The NAS OSI data communications architecture, as defined in FAA-STD-039, includes end-systems and intermediate systems which may be interconnected to form local area and wide area subnetworks. Each subnetwork supports one or more of the subnetwork attachment protocols identified in FAA-STD-039. A subnetwork is typically operated by a specific organization and may be considered a secure environment by that organization as defined by the security policy governing subsystems which form that subnetwork. End-systems interconnecting across the NAS Internet to remote subnetworks have little knowledge of the level of security provided by intermediate subnetworks or the destination subnetwork. Partitioning of the NAS Internet architecture provides a scheme for planning the deployment of OSI security services to optimize protection against OSI communication threats.

This NAS OSI security architecture partitions the NAS Internet into the following three architectural divisions with respect to possible untrusted network elements and the provision of security services:

- Untrusted Local Subnetwork (figure 2)
- Untrusted Intermediate Subnetwork (figure 3)
- Untrusted NAS Internetwork (figure 4)

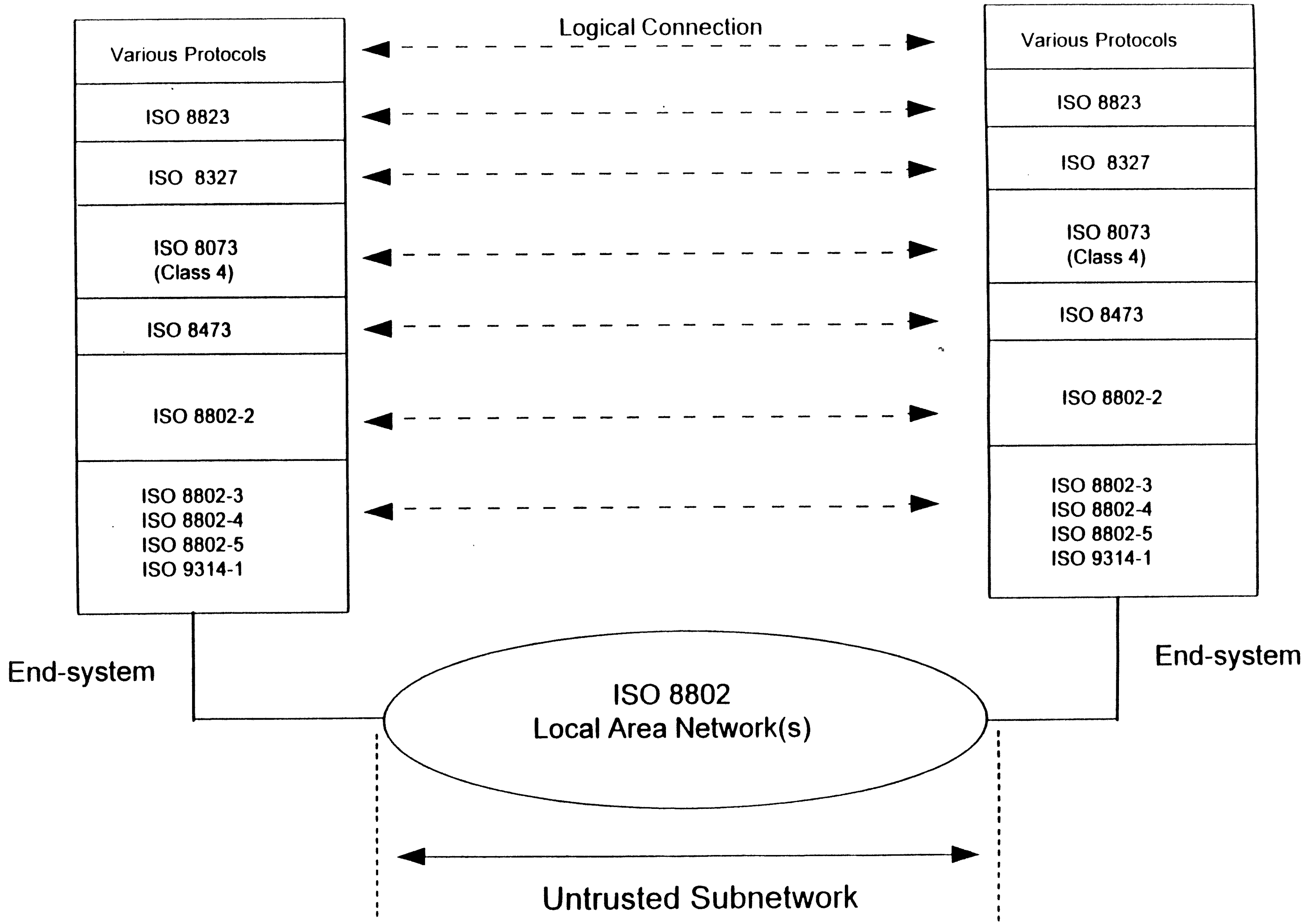
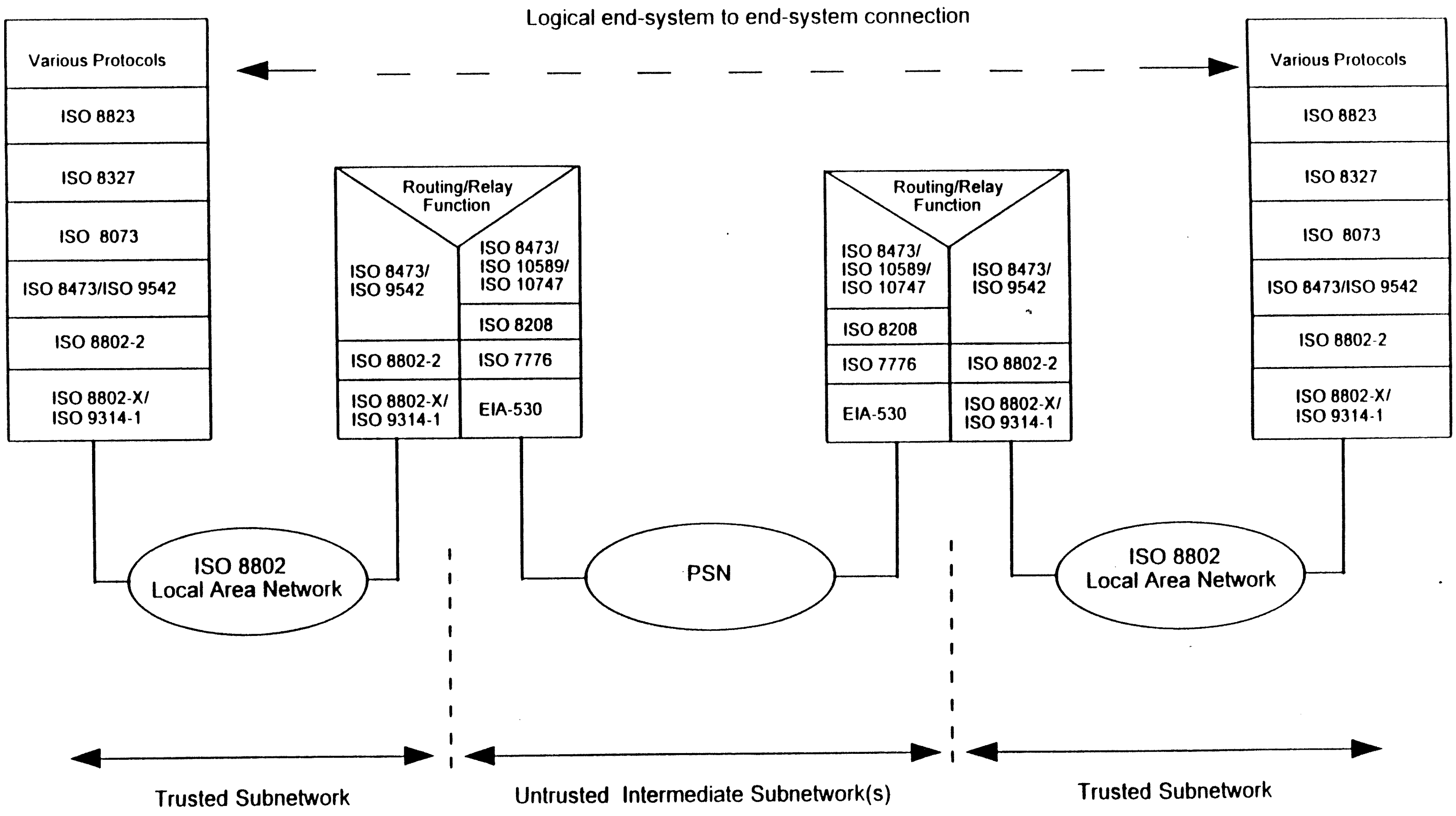
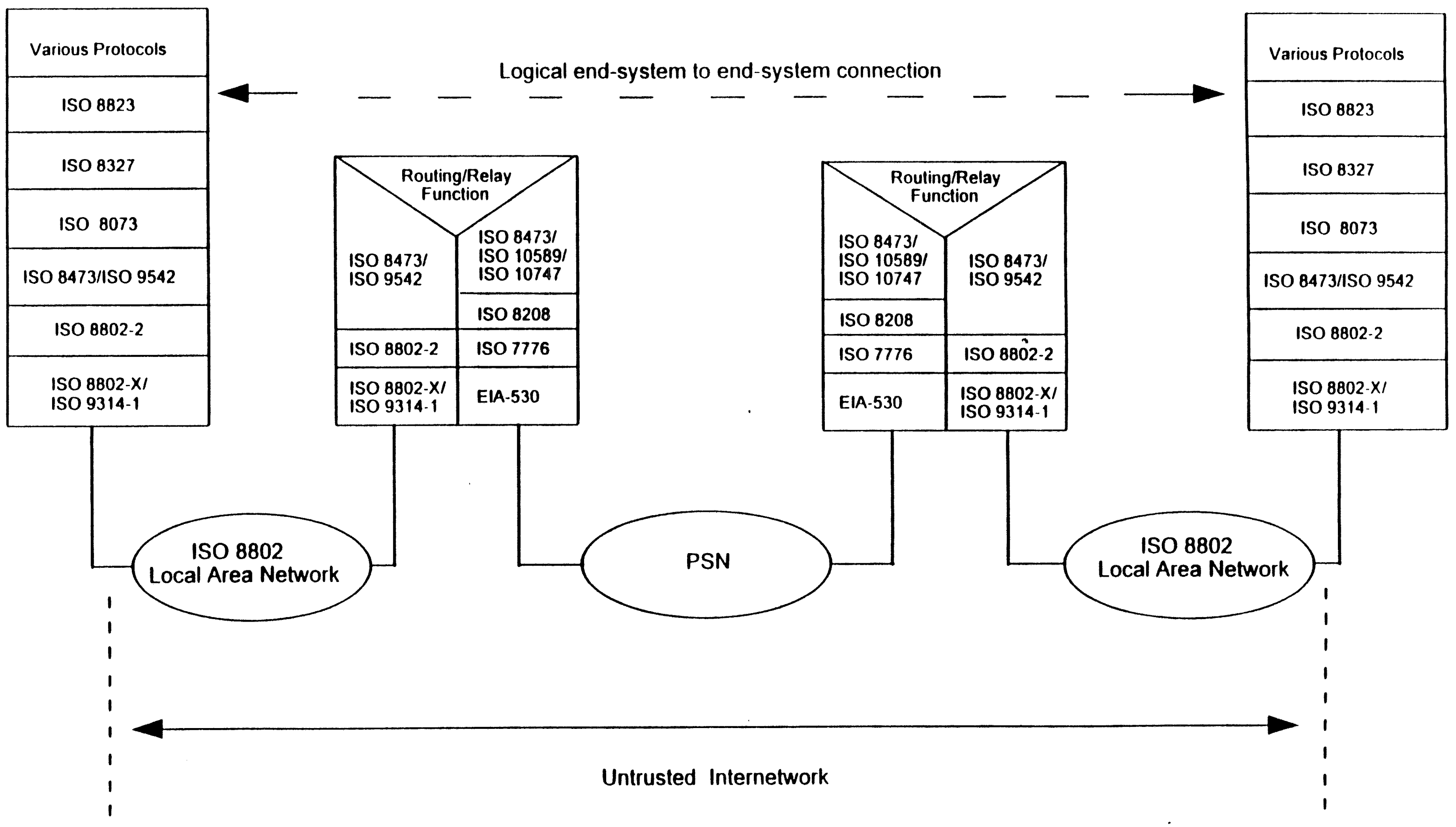


Figure 2 Untrusted Local Subnetwork



ISO 8802-X = ISO 8802-3, ISO 8802-4 or ISO 8802-5

Figure 3 Untrusted Intermediate Subnetwork



ISO 8802-X = ISO 8802-3, ISO 8802-4 or ISO 8802-5

Figure 4 Untrusted Internetwork

OSI security protocols should be selected for implementation depending on which of the above network partitions are deemed untrusted and considered a security threat as well as which services are required to protect the data in transit. For example, consider two or more end-systems connected via an untrusted LAN. If data integrity and authentication services are required for secure communication they would typically be provided by implementing the SDE protocol at the data link layer, which provides the data integrity service, and implementing peer entity authentication services within ACSE at the application layer. These two protocols are described in more detail in sections 3.2.2.1 and 3.2.7.4 respectively.

Table 3.2 indicates the various mappings between NAS systems connected via a LAN or WAN and the applicable OSI security protocols or mechanisms defined in this security architecture. Figures 5, 6, and 7 show the architectural position of the OSI security protocols and services with respect to the NAS WAN and LAN architectures. These figures indicate every NAS OSI security protocol which is applicable to protecting each architechtual configuration. It should be understood that every security protocol may not be required but an informed choice should be made. The following paragraph provides an example of how such choices may be decided.

Consider a hypothetical program office which, following a security risk analysis, decides that their LAN subnetwork requires only two security services: authentication of the application user to prevent unauthorized access to applications and data integrity service to prevent explicit modification by an unauthorized entity. With reference to figure 6 and table 3.1, the hypothetical program office decides to implement the application authentication service using mechanisms specified in ACSE (section 3.2.7.4) and the data integrity service using mechanisms offered in the SDE protocol (section 3.2.2.1). In this case TLSP is not required by the hypothetical program office even though it is present in figure 6. In an alternative scenario the hypothetical program office may have a requirement that end systems communicate securely over both LAN and WAN subnetworks. The security services of application authentication and data integrity are again required. In this case figures 5, 6 and 7 are relevant. The authentication services can be provided again by ACSE but the data integrity service must now be provided by TLSP as it is the only NAS security protocol which provides this service and operates between end-systems, irrespective of the underlying subnetwork type (see table 3.1).

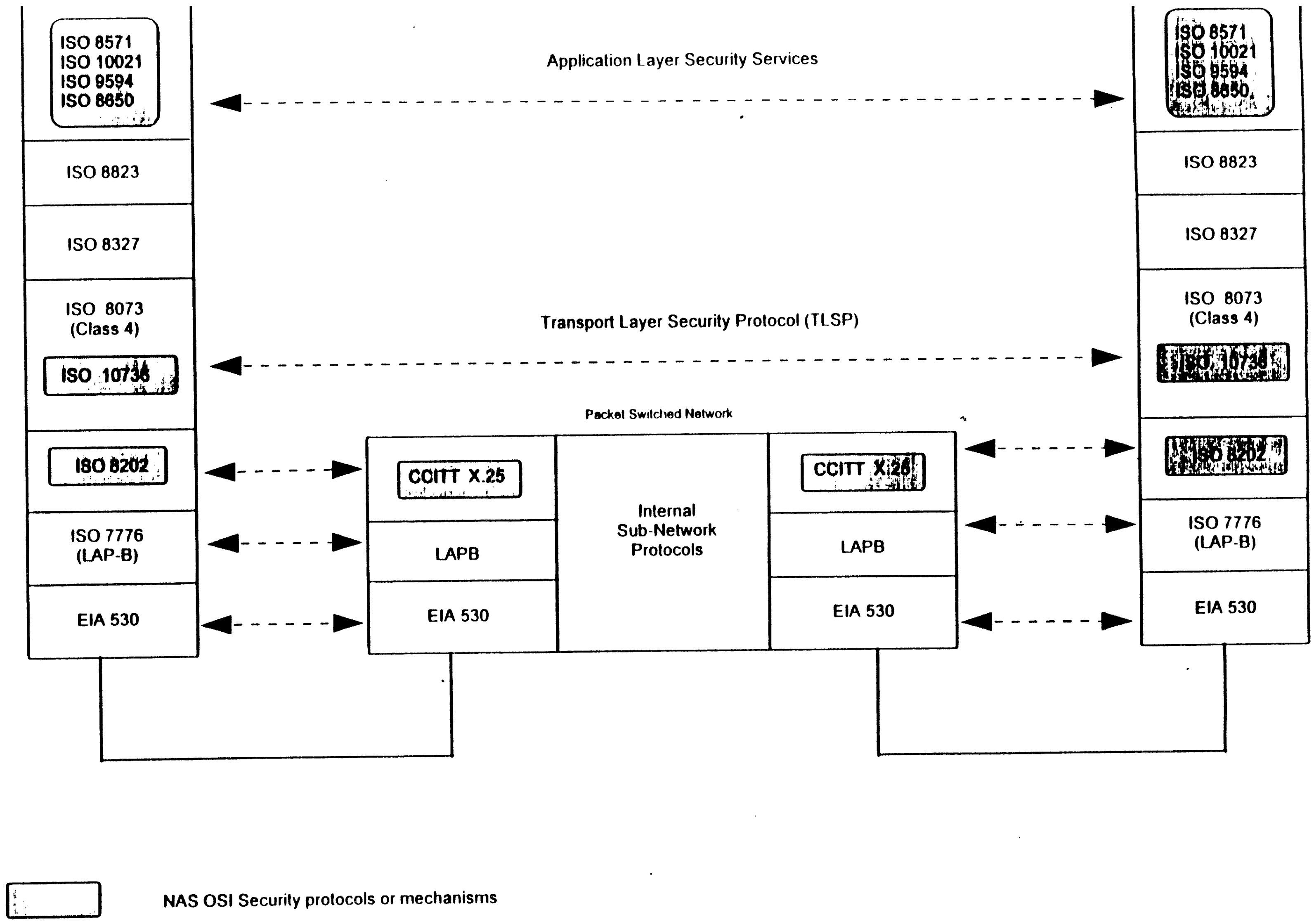


Figure 5 Application of Security Protocols to End-systems connected via PSN

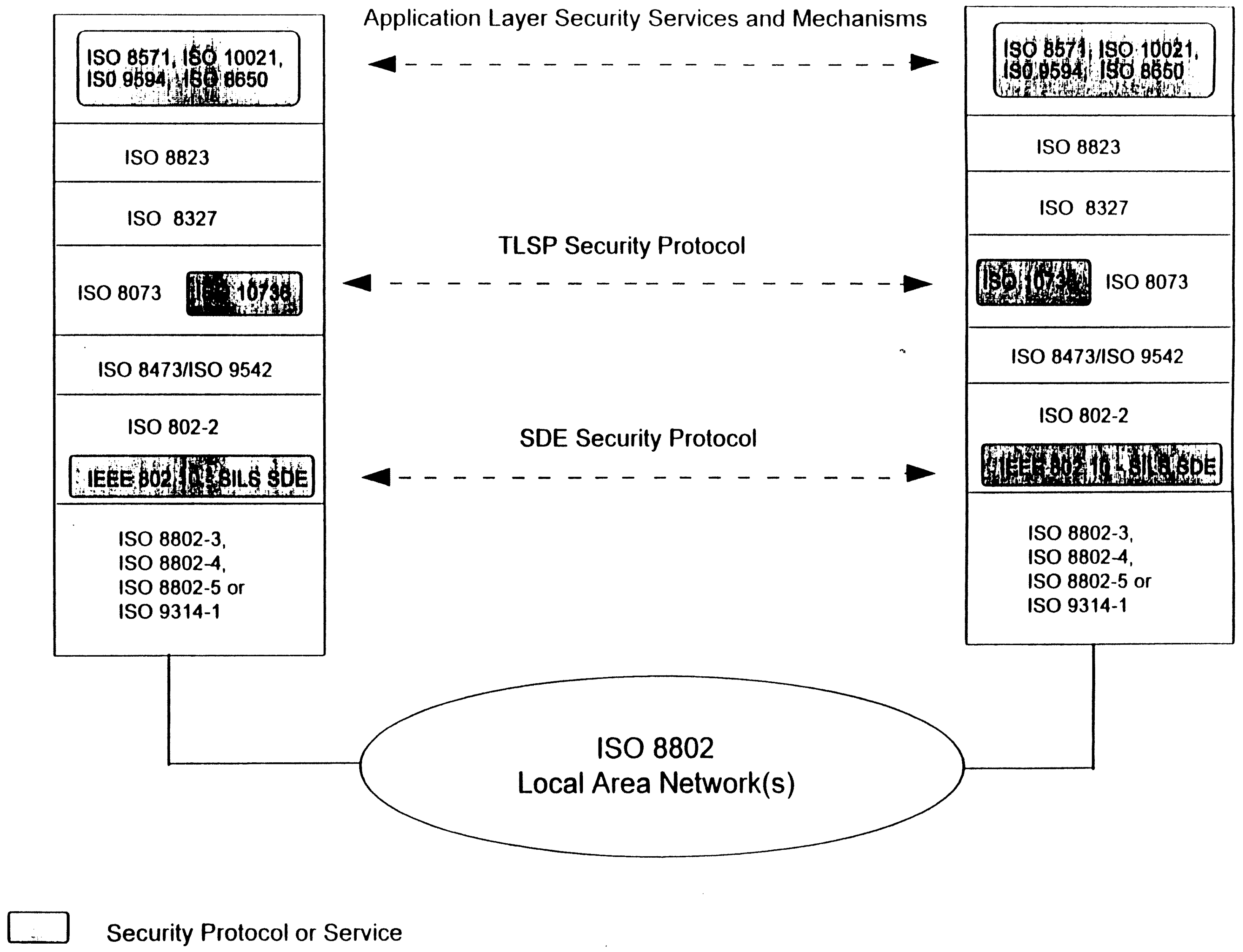


Figure 6 Application of Security Protocols to end-systems connected via Local Area Network

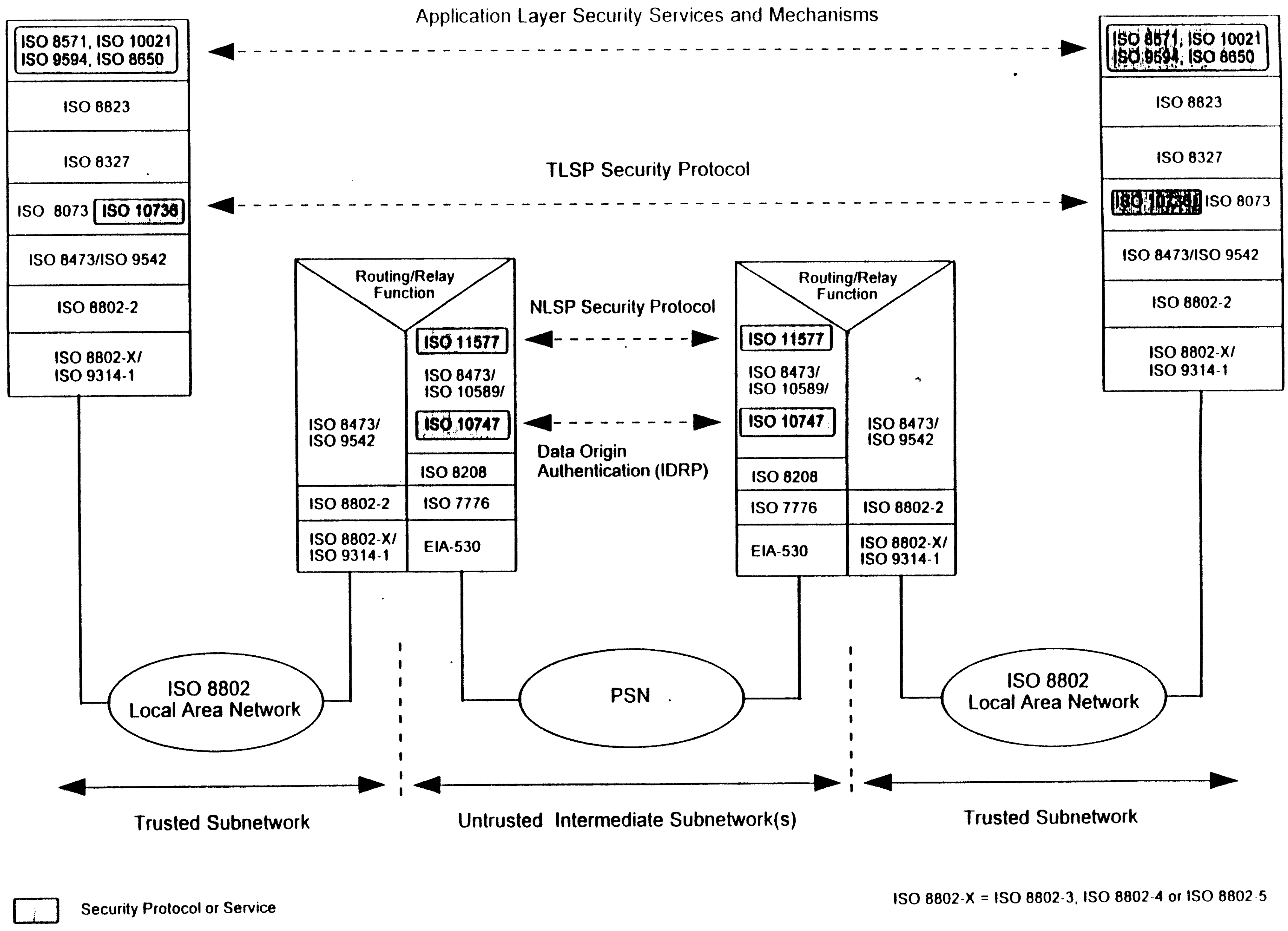


Figure 7 Application of OSI security protocols to intermediate subnetwork

	NAS OSI Security Protocols				
NAS OSI Architecture configurations	Data Link Layer SDE (IEEE 802.10b)	Network Layer NLSP (ISO 11577)	Network Layer CUG/NUI (ISO 8208)	Transport Layer TLSP (ISO 10736)	Application Laye (ISO 8650 ISO 85' ISO 10021, ISO 95
End-systems connecting via LANs	X			X	X
End-systems connecting via PSN			X	X	X
Intermediate systems (Routers)		X			

Table 3.2 NAS OSI Security Services applicable to NAS OSI Architectures

3.1.3 Security Domains within the NAS

The NAS Internet should be sub-divided into security domains which clearly define which organization has responsibility for ensuring the secure transfer of information exchanged within and between specified boundaries (see figure 8). Each organizational security domain should be governed by an organizational security policy which lists mandatory and optional security services that shall be implemented across the domain to protect specified application data. Where applicable, protocols and mechanisms to implement such mandatory and optional services shall be drawn from this standard.

The collection of organizational security domains form the NAS Security Domain and should be governed by a NAS Security Policy. This policy mandates the minimum security requirements to be implemented across all organizational security domains and the security requirements to be placed on NAS Security Domain boundary systems to external networks such as the ATN. The security policy also identifies encipherment algorithms which are applicable for use within the NAS by the security protocols specified in 3.2 of this document. This approach allows a single document to specify one (or more) encipherment algorithm(s) which may be used with OSI security protocols and other non-OSI related security services.

3.1.4 Security Architecture components provided by Network Management Services

All detected attacks on the NAS shall be immediately reported to the network operations personnel for a given security domain as well as recorded in a secure audit trail for future analysis. These functions are most efficiently performed through cooperation with the network management system which is continuously monitoring the network and reporting anomalous events. This security architecture places specific requirements on the network management

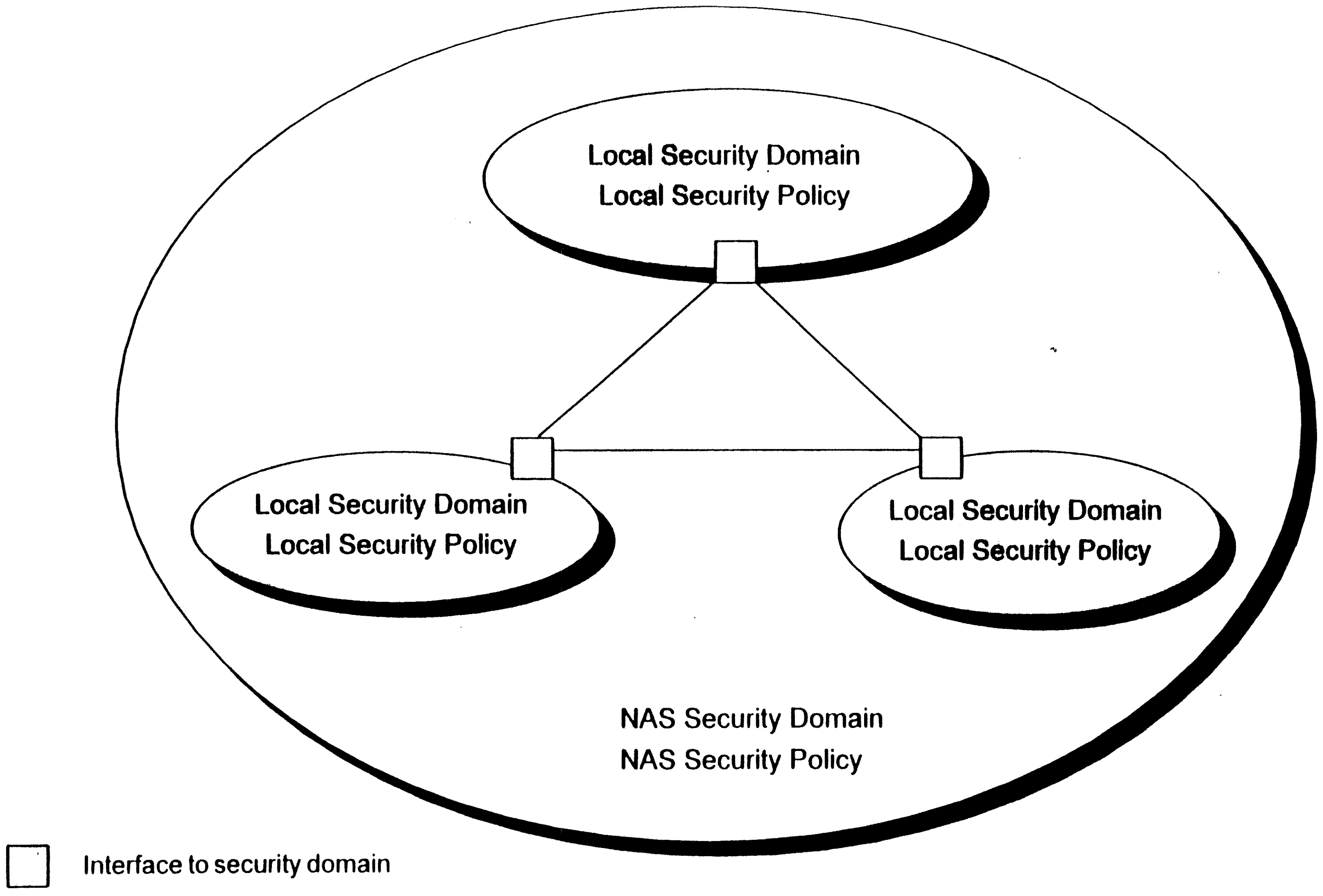


Figure 8 Security Domains within NAS

system for the support of network management services which operate in conjunction with the security protocols and mechanism defined in the standard. Security requirements for the following OSI network management services are specified in section 3.2.8:

- Audit Trail System Management Function
- Security Alarm Reporting Function

3.1.5 Testing of security

Requirements for the testing of NAS security services, protocols and mechanisms will be specified in the next revision of the NAS conformance testing standard FAA-STD-047 as well as the NAS interoperability testing standard FAA-STD-048 currently under development.

3.1.6 Application of Security Protocols to subsystems supporting partial OSI stack

The NAS OSI security architecture can be applied to OSI subsystems which support partial OSI stacks such as 3 layer or 4 layer stacks.

Appendix A illustrates possible security configurations applicable to the four layer category 3 stack defined in NAS-IR-51035101 for connecting remote monitoring subsystems and maintenance processor subsystems.

3.2 NAS OSI Security Services and Protocols

This section specifies requirements for each of the OSI security services, protocols and mechanisms which form part of this standard. Each of the OSI security protocols support a broad range of optional security services and mechanisms. The requirements specified in this section limit the use of these mechanisms to a set that support the NAS security Architecture described in section 3.1. This provides maximum interoperability between OSI security services and also meets the NAS OSI security requirements for NAS OSI end-systems and intermediate systems.

3.2.1 Physical Layer Security

This standard places no requirements on physical layer security protocols or mechanisms.

3.2.2 Data Link Layer Security

Security services specified at the data link layer of this standard are used to protect NAS end-systems connected via 8802-2 based LAN protocols. The security services offered at the data link layer protect application data traversing an untrusted 8802-2 based subnetwork and prevent masquerading and replay from unauthorized entities within the subnetwork.

The following optional security services are provided at the data link layer:

- Data Integrity
- Data Origin Authentication

3.2.2.1 IEEE 802.10(b) Secure Data Exchange Protocol

NAS 8802-2 based end-systems requiring data integrity and data origin authentication services at the data link layer shall implement the Security Data Exchange (SDE) protocol as defined in the IEEE 802.10(b) standard and in accordance with requirements specified in this standard.

The SDE protocol defines a layer 2 entity which operates as part of the ISO 8802-2 Logical Link Control (LLC) sublayer (see figure 1). It provides the following security services across the media access control sublayer: Data confidentiality, Connectionless Integrity, Data Origin Authentication and Access Control. The SDE protocol allows interoperability between stations with and without an implementation of the SDE protocol entity and also operates across LAN bridges implemented in accordance with IEEE 802.1 .

SDE implementations shall, at a minimum, support protocol mechanisms for the Integrity Check Value and the Data Origin Authentication services.

3.2.2.1.1 Integrity Check Value

The Integrity Check Value (ICV) field shall be present in the SDE protocol data unit if requested by the originating SDE user (data link layer user).

The encipherment algorithm for protecting the ICV shall be identified in the security policy for the security domain as described in section 3.1.3 of this document.

The PAD (padding) field shall be supported and used as required by the identified encipherment algorithm.

3.2.2.1.2 Data Origin Authentication

The station-id shall be present within the protected header of the SDE PDU if data origin authentication at layer 2 is requested by the SDE user. The station-id shall include the MAC address of the originating station as specified in IEEE 802.1a.

Authentication of the originating station-id is implicitly performed through the originator's knowledge of the encipherment key used to create the ICV. Therefore users requesting authentication shall also request data integrity and an integrity check value field shall be present in the SDE PDU.

3.2.2.1.3 Interoperability with LAN stations not supporting SDE

If stations supporting SDE are required to interoperate with stations not supporting SDE then all SDE entities shall include the < Clear Header > field within the SDE PDU.

3.2.3 Network Layer Security

Security services at the network layer are provided for the following purposes:

(a) To protect data traversing untrusted intermediate subnetworks.

(b) To protect a subnetwork from entities masquerading as NAS end-systems or NAS intermediate systems.

(c) To protect end-systems directly connected to NADIN PSN from unauthorized access by remote DTEs.

The following optional security services are provided at the network layer:

- Data Integrity
- Data Origin Authentication

These two services provide the two functions of protecting the network protocol data units from undetected modifications as well as establishing a firewall to protect the receiving subnetwork from unauthorized access.

3.2.3.1 Network Layer Security Protocol

NAS intermediate systems requiring data integrity or data origin authentication services at the network layer shall implement the NLSP in accordance with ISO/IEC 11577 and the following requirements:

a) The NLSP connectionless mode of operation (NLSP-CL) shall be supported .

b) The Data Origin Authentication service and/or Connnectionless Integrity service shall be supported. Other services provided by NLSP are outside the scope of this standard.

c) All NLSP service parameters shall be protected by setting the SA (security association) Attribute <Para_Prot> to TRUE. This protects both addressing and user data parameters.

NLSP is a subnetwork independent convergent protocol which operates in conjunction with the ISO 8473 Connectionless Network Protocol (CLNP) to protect CLNP data units traversing an untrusted subnetwork. It is positioned in the NAS security architecture above CLNP as indicated in figure 7. NLSP shall be implemented on 3 layer intermediate systems which provide subnetwork interfaces between a trusted subnetwork and an untrusted subnetwork (e.g. NAS routers). NLSP services shall not be accessible to NAS end systems as equivalent functionality is provided on end-systems using the TLSP protocol described in section 3.2.4.1.

Requirements for using these services shall be specified in the security policy for each security domain.

3.2.3.2 Network layer security between end-systems connected via PSN

End systems connecting via NADIN PSN and requiring access control at the network layer shall use the Closed User Group (CUG) and Network User Identification (NUI) facilities defined within the ISO 8208 standard.

3.2.3.3 ATN Security Label

CLNP implementations in end-systems and intermediate systems shall support the ATN security label as defined in the ATN Manual. This label restricts CLNP traffic to specific routes as defined by the "shell" ATN security policies.

3.2.4 Transport Layer Security

Security Services at the transport layer are used to protect data between end systems when the level of security within the local subnetwork or between subnetwork boundaries is untrusted.

The Transport layer security protocols and mechanism provide the following optional security services:

- Data Integrity
- Data Confidentiality

Techniques for making these services available to the NAS ASEs is a local matter but the recommended mechanism is through the Quality of Service parameter supported within the ISO 8072 transport service standard.

Use of each service depends on the requirements of the NAS application and the security polices which govern the end-system's security domain. Each service shall be provided on a transport connection basis to allow flexible and efficient use by the upper layer application.

Security services offered at the transport layer may be used to support Request/Response type NAS applications which exchange application messages and require end-to-end data confidentiality and data integrity.

3.2.4.1 Transport Layer Security Protocol

NAS open end-systems requiring data confidentiality or data integrity services at the transport layer shall implement the TLSP as defined in ISO/IEC 10736 and in accordance with the requirements defined in this standard.

TLSP shall be used in conjunction with the ISO Transport Protocol (ISO 8073) to protect transport protocol data units (TPDUs) sent between NAS end-systems.

Transport layer multiplexing shall be implemented to allow the selection of differing security protection services for differing transport connections while allowing a network connection to be shared.

The security padding function shall be supported and used as required by the selected encryption mechanism.

If the Integrity Check function is selected then the ICV must be encrypted using the encryption algorithm identified in the NAS OSI Security Policy. The ICV key granularity shall be selected to provide separate cryptographic keys for each transport end-system pair (ICV_Kg = Kg_esp).

An Agreed Set of Security Rules (ASSR) shall be defined for use with the data integrity check function and the data encipherment function. The ASSR shall be assigned unique object-identifiers which allow the ASSR for a specific transport connection to be identified via the layer 7 Security Exchange Service Element.

3.2.5 Session Layer Security

This standard places no requirements on session layer security protocols or mechanisms.

3.2.6 Presentation Layer Security

This standard places no requirements on presentation layer security protocols or mechanisms.

3.2.7 Application Layer Security

This section describes the Application layer security protocols and mechanisms identified for use within NAS open end-systems.

3.2.7.1 Application Layer Security Services

The following security services are provided at the Application layer of the NAS OSI Security Architecture:

- Authentication.
- Discretionary Access Control.

Layer 7 security services are primarily focused on authenticating the identity of NAS OSI application processes attempting to establish peer associations. Authentication information shall be protected using encipherment mechanisms as described in section 3.2.7.4 below.

The Association Control Service Element is the ASE used for exchanging generic authentication information between all NAS OSI application service elements. It may optionally be used in conjunction with the ISO/IEC 9594-8 Directory Authentication Framework to provide a secure authentication service to all NAS OSI ASEs. Selected NAS ASEs may include additional authentication parameters which may be optionally used as required (e.g.: FTAM see section 3.2.7.2).

Layer 7 discretionary access control services are provided by selected NAS OSI ASEs that support appropriate access control services and mechanisms (e.g. FTAM and Directory Services). This standard defines no additional access control requirements on such ASEs beyond those defined in FAA-STD-039.

The Message Handling Services ASE supports a superset of the security services required within this standard and is treated separately in section 3.2.7.3

3.2.7.1.1 Accessing Lower Layer Security Services

A NAS ASE may require security services provided at the Lower Layers (Transport Layer or below) in order to ensure its data is securely transferred across the NAS Internet. For example FTAM may require the use of data confidentiality services offered at the Transport Layer by TLSP. Communication of such requirements within an end-system is a local matter but the QOS (Quality of Service) parameter is the recommended mechanism for requesting services from the lower layers.

Each NAS ASE using security services shall define an Agreed Set of Security rules (ASSR) which describe which of the security services and options outlined in this standard shall be required and operational in order to establish a connection with the ASE. Selected encipherment algorithms shall be included in the rules. This information may be used both to configure security protocols and mechanisms in NAS OSI systems as well as in conjunction with the QOS parameter to request appropriate security services.

3.2.7.2 File Transfer Access and Management (FTAM)

3.2.7.2.1 Authentication

NAS open end-systems requiring authentication services defined within the File Transfer Access and Management standard shall implement the < initiator-identity > and < filestore password > parameters in accordance with the ISO 8571 FTAM. These parameters shall be encrypted using the encipherment algorithm identified in the NAS security policy governing that systems security domain.

3.2.7.2.2 Discretionary Access Control

NAS OSI systems requiring discrétionary access control services within FTAM shall implement the Security Attribute Group in accordance with ISO 8571. The < identity > and < location > components of the Access-Control-Element shall be supported by FTAM initiators and responders. The identity field shall be used to identify FAA personnel wishing to transfer or access remote files and the < location > component shall be used to identify application process wishing to transfer or access remote files automatically. An application process shall be identified by an Application Entity Title as defined in FAA-STD-042.

Use of the < passwords > component of the Access-Control-Element is not recommended due to the excessive number of passwords which must be managed for each filestore and remembered by users of the file. Use of Authentication mechanisms described above are recommended for this purpose.

3.2.7.2.3 Data Confidentiality

FTAM does not define data confidentiality services for use in transferring file data units. NAS end-systems requiring this service shall use the data confidentiality mechanisms defined in the transport layer security protocol (see section 3.2.4).

3.2.7.3 Message Handling System (MHS)

3.2.7.3.1 NIST Security Classes

The ISO 10021 (MHS) standard defines a broad set of security services which exceed the identified NAS OSI security requirements. The NIST Implementation Agreements (SP-500-214) group these security services into six security classes which protect the nine possible interfaces between the MHS system components (User Agent, Message Transfer Agent and Message Store). Within the NAS security architecture, MHS is treated as a self contained application service which shall provide all the security services required by its user. This is because of its store and forward mode of operation and the possibilities for transferring MHS messages through external service providers.

3.2.7.3.2 Encipherment Algorithms

Security services requiring an encipherment mechanism shall use the encipherment algorithm identified in the organizational security policy for the local security domain of interest or the NAS security policy depending on the scope of the MHS implementation within the NAS.

3.2.7.4 Association Control Service Element (ACSE)

Peer entity-authentication shall be supported during association establishment as specified in Addendum 1 to ISO 8650 Association Control Service Element. Optionally the ISO/IEC 9594-8 Directory Authentication Framework may be used as an authentication mechanism. If so then the following requirements apply:

(1) The "Credentials" parameter, as defined in ISO/IEC 9594-8 shall be the "Authentication-Value" exchanged by AARQ and AARE protocol data units of ACSE. . The "DistinguishedName" field of this parameter shall identify the Application Entity Title using the Directory Information Tree naming conventions identified in FAA Naming and Addressing Standard FAA-STD-042.

(2) Either *simple authentication* or *strong authentication* mechanisms may be used depending on the level of security required by the application.

(3) When implementing *simple authentication* the "DistinguishedName" and "Password" shall be protected using an encryption algorithm (hash function) identified in the NAS OSI Security Policy.

(4) When implementing *strong authentication* the public key algorithm and issuing certification authority shall be used as identified in the NAS OSI Security Policy. Either a one-way authentication exchange or two-way authentication exchange may be implemented as required by the NAS application. Three-way authentication exchanges are outside the scope of this standard.

The authentication mechanisms described in this standard requires the availability of an ISO 9594 Directory Service which maintains "DistinguishedName" and "Password" pairs for NAS applications and performs the authentication mechanism on behalf of a requesting application. The directory may also be used as the repository for public keys (certificates) used by *strong authentication* mechanisms.

3.2.8 Network Management and Security

This section describes network management services and functions which are required in support of this security standard. This includes provision of security audit trails and security alarm functions.

Network management services and functions will be responsible for reporting attacks detected by security protocols and mechanisms as well as monitoring and recording operations performed on security related objects.

3.2.8.1 Audit Trail of Network and System Management Resources

The Audit trail service shall be provided by the Audit Trail System Management Function as defined within the OSI Network Management Standard (ISO 10164-8). The following events shall produce notifications which result in an event report being logged in the audit trail:

- Use of Authentication mechanisms.
- Actions performed by Computer Operators/System Administrators
- Actions performed by system security officers.
- Notifications of attempted breaches in security services described in this standard.
- Notification of successful breaches in security services and mechanisms described in this standard.
- Creation and Deletion of security related managed objects.

For each event reported the following information shall be recorded:

- Date and time the event occurred
- User or Process which initiated the event including network location address
- Type of the event
- Success or failure of the event
- Name of any managed objects which are created or deleted

The information repository containing audit trail records shall be protected from unauthorized network access using authentication and access control mechanisms. This information repository must also be protected from unauthorized local access by storing it on a trusted computing base which adheres to FAA security requirements for host computer environments.

3.2.9 Relationship to ATN Security Requirements

The ATN manual defines the OSI end-system and intermediate system requirements for connecting over the ATN. The current ATN requirements include provisions for the ATN security label. The NAS OSI security standard is aligned with these requirements as described in section 3.2.3.3 of this document. This standard will be updated as further ATN security requirements are developed.

4. QUALITY ASSURANCE PROVISION

This section is not applicable to this standard.

5. PREPARATION FOR DELIVERY

This section is not applicable to this standard.

6. NOTES

6.1 Definitions

END SYSTEM: An end system (ES) contains the application processes that are the ultimate sources and destinations of user oriented message flows. The functions of an end system can be distributed among more than one processor/computer. End systems are sometimes referred to as Hosts.

INTERMEDIATE SYSTEM: An intermediate system (IS) interconnects two or more subnetworks. For example, it might connect a local area network with a wide area network. It performs routing and relaying of traffic. A processor can implement the functions of both an end system and an intermediate system.

OPEN SYSTEM: FIPS Pub 146-1 defines an open system as a system capable of communicating with other [open] systems by virtue of implementing common international standard protocols. However, an open system may not be accessible by all other OSI systems. This isolation may be provided by physical separation or by technical capabilities based upon computer and communications security.

NETWORK SECURITY: The protection of networks and their services from all natural and human-made hazards. Provides an assurance that the network performs its critical functions correctly and that there are not harmful side-effects.

NAS SPECIFIC ASE: A Layer 7 NAS Application which makes use of the upper layer OSI services and interfaces directly to ACSE rather than invoking an existing OSI ASE such as FTAM or Directory Services.

PROTOCOL: In the Open Systems Interconnection reference model, the communication functions are partitioned into seven layers. Each layer, N, provides a service to the layer above, N+1, by carrying on a conversation with layer N on another processor. The rules and conventions of that N-layer conversation are called a protocol.

RISK: The loss potential that exists as the result of threat and vulnerability pairs. Reducing either the threat or the vulnerability reduces the risk.

SECURITY: Mechanisms and techniques that control access to system assets. Protection is against, for example, unauthorized modification, destruction, denial of service or theft.

SECURITY DOMAIN: An organizational group/subgroup with a defined security policy. The FAA Security Domain is regulated by the FAA Automated Information Systems Security Policy and the FAA Telecommunications Security Policy (Draft).

SECURITY POLICY: The set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information.

SENSITIVITY/CLASSIFICATION: A determination that information requires a specific degree of protection against unauthorized access together with a designation signifying that such a determination has been made. Classification is performed according to a stated policy.

THREAT: A potential violation of system security.

TRUSTED COMPUTER SYSTEM:A system that employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

TRUSTED COMPUTING BASE (TCB):The totality of protection mechanisms within a computer system (including hardware, firmware and software) the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

TRUSTED SUBNETWORK: The totality of protection mechanisms within a partitioned network of computer systems the combination of which is responsible for enforcing a security policy across the boundaries of that subnetwork.

UNTRUSTED SUBNETWORK: A subnetwork whose protection mechanisms are considered insufficient for providing the secure exchange of unprotected data. This may be due to an unknown or insufficient security policy governing this subnetwork.

SECURITY SERVICE: A service represents a set of functions offered to a user (typically a computer system or a computer communications system). A security service represents those sets of security functions offered to a user.

SECURITY MECHANISM: A security mechanism is a technique or method that when implemented reduces a known security risk.

6.2 Acronyms and Abbreviations

AARE:	A-Associate-response
AARQ:	A-Associate-request
AE:	Application Entity
AP:	Application Process
ATC:	Air Traffic Control
ANSI:	American National Standards Institute
ASE	Application Service Element
ASN:	Abstract Syntax Notation
ASSR	Agreed Set of Security Rules
ATN:	Aeronautical Telecommunications Network
CCITT:	International Telephone and Telegraph Consultative Committee
CLNP:	Connectionless Network Protocol
EIA:	Electronic Industry Association
ES:	End System
FAA:	Federal Aviation Administration
FTAM:	File Transfer, Access and Management
GOSIP:	Government Open Systems Interconnection Profile
ICV:	Integrity Check Value
ISO:	International Organization for Standardization
ICAO:	International Civil Aviation Organization
IEEE:	Institute of Electrical and Electronic Engineers
IS:	Intermediate System
LAN:	Local Area Network
LCN:	Local Communications Network
LLC:	Logical Link Control
MHS:	Message Handling Service (X.400)
NADIN:	National Airspace Data Interchange Network
NAS:	National Airspace System
NIST:	National Institute of Standards and Technology
NLSP	Network Layer Security Protocol
NLSP-CL	Network Layer Security Protocol connectionless

NSAP:	Network Service Access Point
OSI:	Open Systems Interconnection
OSIE:	Open Systems Interconnection Environment
P-Selector:	Presentation Selector
PSN:	Packet Switched Network
PDU:	Protocol Data Unit
QOS:	Quality of Service
S-Selector:	Session Selector
SDE:	Secure Data Exchange
SNPA:	Subnetwork Point of Attachment
SAP:	Service Access Point
SILS:	Standard for Interoperable Local Area Network Security (SILS)
SnPA:	Subnetwork Point of Attachment
TLSP:	Transport Layer Security Protocol
TNB:	Trusted Network Base
TPDU:	Transport Protocol Data Unit
T-Selector:	Transport Selector
WAN:	Wide Area Network

Appendix A

Example of Security Configuration Applicable to Partial OSI Stacks

The NAS OSI security architecture can be applied to OSI subsystems which support partial OSI stacks such as 3 layer or 4 layer stacks.

This appendix describes possible security configurations applicable to the four layer category 3 stack defined in NAS-IR-51035101 for connecting remote monitoring subsystems and maintenance processor subsystems. Figure B illustrates how the transport layer security protocol may be used to provide end-system to end-system security services as discussed in section 3.2.4.1. Also, as the sub-network attachment protocols is ISO 8208, then its closed user group security mechanism may be used to prevent network access from unauthorized end-systems.

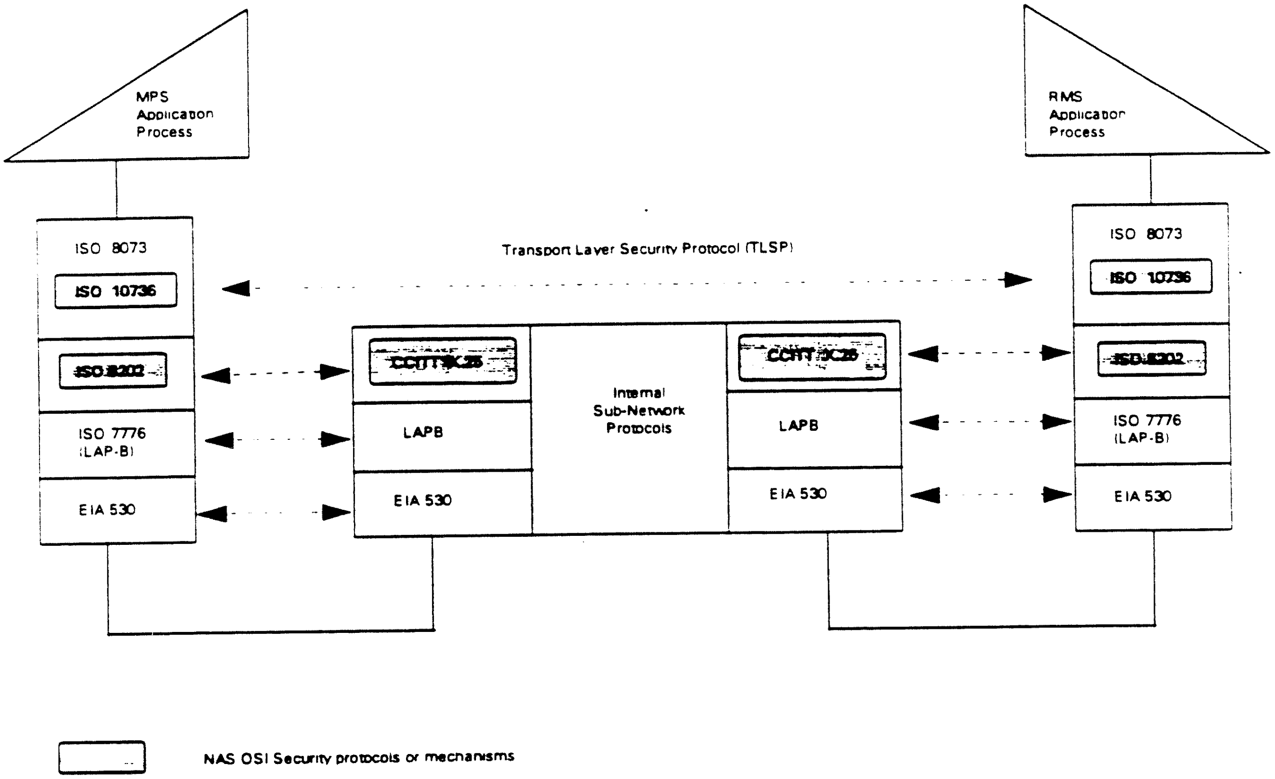


Figure B Example Application of NAS Security Protocols to RMS/MPS Subsystems

Appendix B

Rationale behind FAA-STD-045 Security Decisions

This appendix describes how each of the following eight derived NAS communications security requirements (see 1.3) shall be supported within the NAS OSI security architecture by using selected options from the OSI security protocols identified in the body of this standard. Unless otherwise specified each service is described in terms of either securing the end-to-end connection between end-systems, securing the subnetwork itself or securing the network layer routers between untrusted subnetworks.

B.1 NAS Data Integrity Services

Data integrity within this security architecture shall be supported for the three security partitions described in section 3.1.2 by using data integrity services at the Data link layer, Network or Transport layer as described in the sections below.

Support for services at each layer is optional but transport protocol data units with a destination NSAP address which is external to the security domain of the source subnetwork must be protected using either network layer or transport layer data integrity services as defined below.

B.1.1 Data Integrity within the subnetwork

If the LAN subnetwork is deemed susceptible to data corruption due to deliberate unauthorized modification, reordering or substitution of data traffic or non-deliberate data corruption due to error then the connectionless integrity services of the Secure Data Exchange protocol (IEEE 802.10b) shall be implemented at the data link layer of the 8802-2 based subnetwork. This provides an encrypted corruption detection based integrity service which operates across 8802-2 bridges within the subnetwork. If the subnetwork consists of subnetwork attachment protocols not using 8802-2 logical link control then data integrity services should be placed at the transport layer as discussed B.1.3 below.

B.1.2 Data Integrity at the Subnetwork boundary

If intermediate subnetworks or subnetwork routers are deemed susceptible to deliberate or non deliberate data corruption then the data integrity service of the Network Layer security Protocol shall be used across untrusted subnetworks as indicated in figure 3. This results in an encrypted seal being append to the network protocol data unit. This architecture shall require use of the connectionless mode of the NLSP so that it may operate in conjunction with NSAP address of the connectionless network protocol.

Typically, a high percentage of NAS network traffic will be local to a subnetwork. If this subnetwork is considered secure from data corruption; then only apply data integrity services to data with an external subnetwork destination as indicated by its NSAP address. This approach reduces the additional processing overhead caused by data integrity mechanisms. Use of NLSP within the subnetwork router allows the network administration authority to take responsibility for ensuring implementation and use of data integrity services. This should be compared to placing these services at the Transport layer of the end-system where the choice of use is removed from the network administration authority and given to the application.

B.1.3 Data Integrity Between End-Systems

The responsibility for applying data integrity services may be moved to the end system. In this case the data integrity mechanisms within the Transport Layer Security Protocol (TLSP) shall be used. The TLSP data integrity services are very similar to those offered by the network layer security protocol, but its position in the OSI architecture places responsibility and control within the end system. This provides a finer granularity of control as selected transport connections may perform integrity checks as requested by the layer 7 application via the Quality of Service parameter.

It should be noted that TLSP integrity services do not protect network protocol parameters, particularly source and destination NSAP addresses, from malicious tampering. This requires use of NLSP at the network layer.

B.2 NAS Data Confidentiality Services

The requirement for data confidentiality is dependent on the value of the information being transmitted. This decision should be described in a security policy. On-line identification and control of confidential information is the responsibility of application layer processes. For the selective encryption of confidential information the data confidentiality service must reside in the end-system. Due to the size and request/response operation mode of a large percentage of the NAS messages, this security architecture requires the use of the data confidentiality services within the Transport Layer Security Protocol. This allows selected transport connections to carry confidential traffic as requested by the application process through the QOS (Quality of Service) parameter.

B.3 NAS Authentication Services

This architecture defines two authentication categories as follows:

- Authentication of application processes
- Authentication of communication end systems

B.3.1 Authentication of Application Processes and Personnel

Application processes shall be authenticated at the application layer using two components:

a) Application Entity Title

b) Password

The Application Entity Title will be a unique identifier of the application process as defined in FAA-STD-042 Naming and Addressing.

Personnel authentication shall also take place at the application layer using two components of:

a) Personnel identifier

b) Password

The personnel identifier component is yet to be defined in the NAS environment and its use will depend on the requirement to connect human entities to remote networked services via the NAS OSI communication protocols.

The password component shall be protected to prevent possibilities of line eavesdropping or replay.

B.3.2 Authentication of Communications Systems

The layer 2 Security Data Exchange (SDE) protocol provides a data origin authentication mechanism as a side effect of support for the data integrity service. This mechanism will authenticate the originating station id of a LAN based end-system using its media access control (MAC) address. This mechanism is less effective and more restrictive than application layer authentication mechanisms described in 3.2.7.1. This is because it only operates within an 8802-2 based subnetwork and is based on knowledge of an encryption key. It shall therefore be optionally supported within NAS subnetworks. LAN end-systems which do not support SDE can interoperate with receiving systems which support SDE allowing transparent support of this security feature among a closed community of end-systems.

B.3.3 NAS Discretionary Access Control Services

Discretionary access control shall be used to control or limit personnel or application processes from gaining access to target objects such as files or data bases. Access control mechanisms provide for varying granularity of access as defined by a specific access control policy defined and governed by the security domain administration.

The access control policy may define individual, group based, role based, multi-level or some other approach to organizing how initiating entities access the target object. This standard does not define the access control policy or the access control decision functions used to enforce this policy. Definition of these features shall be local to a security domain.

This standard will define the authentication information which must be provided by the initiating entity for use by the target entity when performing the access control decision. This authentication information is discussed in section B.3.1.

B.3.4 NAS Object Reuse Services

Requirements for prevention of unauthorized or accidental reuse of objects within the end system are a local implementation requirement which cannot be supported by external OSI communication functions. This requirement shall be met through local implementation mechanisms. External testing performed across the OSI connection shall ensure object reuse mechanisms are implemented successfully.

B.3.5 NAS Audit Trail of Network and System Management Services

Security violations must be recorded in a secure location for future analysis. To achieve this goal, all security services and mechanisms must be closely coupled with a monitoring mechanism which is continually monitoring network activity. Such a monitoring system is required to perform the following tasks:

a) Report security alarms to the network operator for immediate action

b) Log security alarm information in a secure audit trail.

These functions will be most, efficiently performed by the network management system which may be closely coupled to the OSI security protocols and mechanisms through the implementation of appropriate managed objects. The evolving FAA Network Management standard will define protocols services and managed objects to be implemented within the NAS. This security standard defines a set of network management requirements which define minimal services required to complement the NAS OSI Security Architecture. The provision of OSI functions and services to meet these requirements shall be described in the FAA Network Management standard.

B.3.6 NAS System Architecture

Requirements on system software relating to modification of code, data structures or other internal objects are outside the scope of this standard. These requirements should be identified in a standard which defines security requirements for components within an end-system (as opposed to across an OSI communications connection).

B.3.7 NAS System Integrity Service

Requirements for hardware and software functions which periodically validate the correct operation of the end-system are outside the scope of this document. These requirements should be identified in a standard which defines security requirements for components within an end-system (as opposed to across an OSI communications connection). All unrecoverable system integrity errors must be reported via the network management system. All system integrity errors should be recorded in the audit trail for that end system.

B.3.8 Network congestion control and Non-blocking

A network event which prevents the throughput of end-system traffic is an immediate threat to the security because security related traffic (security alarms or audit trail information) may be affected. The implementation of network design algorithms and services which prevent network congestion and blocking shall be implemented within all subnetworks which comprise a security domain. This standards does not define additional protocols or services for avoiding these two conditions.